

# PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-341749

(43)Date of publication of application : 08.12.2000

(51)Int.Cl.

H04Q 7/38

(21)Application number : 11-149548

(71)Applicant : NTT DATA CORP

(22)Date of filing : 28.05.1999

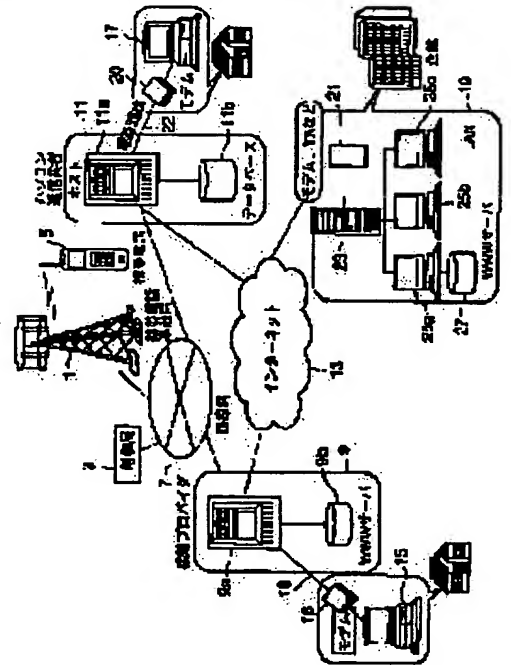
(72)Inventor : ENDO HIDENORI  
KUWAE HITOSHI

## (54) METHOD AND SYSTEM FOR MANAGING CONNECTION OF MOBILE TERMINAL

### (57)Abstract:

**PROBLEM TO BE SOLVED:** To prevent the occurrence of the so-called impersonated connection by a third person illegally acquiring the user ID or password of a terminal owner.

**SOLUTION:** When a connection request to a line is outputted from a portable telephone set 5, a server 23 acquires user ID, a password and a zone number showing the current position of the telephone set 5 from the set 5. Then the server 23 reads out a remote access user management table and respectively compares the user ID, the password and the zone number with registered user ID, password and zone number. Only when all the data completely coincide with each other, the server 23 permits the telephone set 5 to be connected to a remote access point of a LAN 19. If any one of data does not coincide with its reference data, the connection is rejected.



(19) 日本国特許庁 (JP)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開 2000-341749

(P 2000-341749A)

(43) 公開日 平成12年12月8日 (2000.12.8)

(51) Int. Cl. 7

H04Q 7/38

識別記号

F I

H04B

7/26

109

S

テーマコード (参考)

5K067

審査請求 未請求 請求項の数 11 O L

(全10頁)

(21) 出願番号 特願平11-149548

(22) 出願日 平成11年5月28日 (1999.5.28)

(71) 出願人 000102728

株式会社エヌ・ティ・ティ・データ

東京都江東区豊洲三丁目3番3号

(72) 発明者 遠藤 秀則

東京都江東区豊洲三丁目3番3号 株式会社

エヌ・ティ・ティ・データ内

(72) 発明者 桑江 均

東京都江東区豊洲三丁目3番3号 株式会社

エヌ・ティ・ティ・データ内

(74) 代理人 100095371

弁理士 上村 輝之

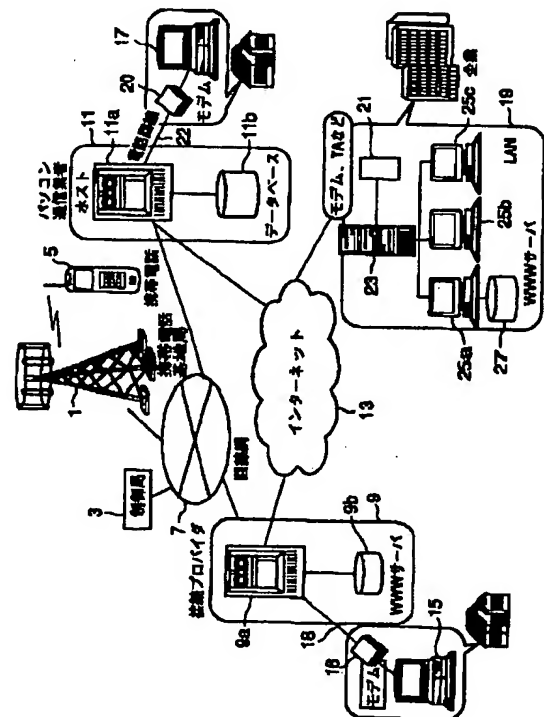
最終頁に続く

(54) 【発明の名称】 モバイル端末の接続管理方法及び方式

(57) 【要約】

【課題】 端末所持者のユーザIDやパスワードを不正に入手した第三者による所謂なりすましの接続を防止できるようにする。

【解決手段】 サーバ23は、携帯電話機5から回線への接続要求があると、携帯電話機5からユーザID、パスワード、携帯電話機5の現在位置を示すゾーンナンバを取得する。リモートアクセスユーザ管理テーブルを読み出し、上記ユーザID、パスワード、及びゾーンナンバと、登録されているユーザID、パスワード、及びゾーンナンバとを夫々比較する。それらが全て一致しているときのみ、携帯電話機5に対しLAN19のリモートアクセスポイントへの接続を容認する。いずれか1つでも不一致のものがあれば、上記接続を拒否する。



## 【特許請求の範囲】

【請求項 1】 移動通信網を通じて送信されるモバイル端末の位置情報を受付ける手段と、  
回線への接続を許可し得る前記モバイル端末の位置情報を記憶する手段と、  
前記受付けた位置情報と前記記憶される位置情報とを比較して、両者が一致するとき前記モバイル端末に対し回線への接続許可を与える手段と、  
を備えるモバイル端末の接続管理方式。

【請求項 2】 請求項 1 記載の方式において、  
前記各手段が、企業内ネットワークを構成するサーバに備えられるモバイル端末の接続管理方式。

【請求項 3】 請求項 1 記載の方式において、  
前記モバイル端末が、携帯電話機、PHS 端末、モバイルコンピュータを含むモバイル端末の接続管理方式。

【請求項 4】 請求項 1 記載の方式において、  
前記位置情報が、移動通信網を形成する基地局のゾーンを示すゾーンナンバで表されるモバイル端末の接続管理方式。

【請求項 5】 請求項 4 記載の方式において、  
前記ゾーンナンバが、前記モバイル端末から最寄りの基地局に無線送信されたモバイル端末自身の位置情報に基づき、専用の交換局において生成されるモバイル端末の接続管理方式。

【請求項 6】 請求項 5 記載の方式において、  
前記ゾーンナンバが、移動通信網を形成する制御局から企業内ネットワークを構成するサーバに送信されるモバイル端末の接続管理方式。

【請求項 7】 請求項 1 記載の方式において、  
前記記憶手段が、前記位置情報と共に、前記モバイル端末のユーザ ID、パスワード、移動機 ID をテーブル形式で記憶しており、前記接続許可付与手段が、前記モバイル端末から送信されるユーザ ID 及びパスワードと、前記記憶されているユーザ ID 及びパスワードとが夫々一致したとき、前記両位置情報の一致／不一致を判定するモバイル端末の接続管理方式。

【請求項 8】 移動通信網を通じて送信されるモバイル端末の位置情報を受付ける手段と、  
回線への接続を許可し得る前記モバイル端末の位置情報と、それに対応するユーザ ID とを、少なくとも 1 人のユーザに対し 2 以上記憶する手段と、  
前記記憶される位置情報中から前記受付けた位置情報に一致するものを選択すると共に、その位置情報に対応するユーザ ID を、発信時に使用すべきユーザ ID として前記モバイル端末に送信する手段と、  
を備えるモバイル端末の接続管理方式。

【請求項 9】 請求項 8 記載の方式において、  
前記モバイル端末からのパスワードと予め登録されるパスワードとが一致したとき、前記モバイル端末に対し回線への接続許可を与える手段を更に備えるモバイル端末

の接続管理方式。

【請求項 10】 請求項 8 又は請求項 9 記載の方式において、  
前記各手段が、パソコン通信業者又はインターネットの接続プロバイダのホスト装置に備えられるモバイル端末の接続管理方式。

【請求項 11】 移動通信網を通じて送信されるモバイル端末の位置情報を受付ける第 1 の過程と、  
回線への接続を許可し得る前記モバイル端末の位置情報を記憶する第 2 の過程と、  
前記受付けた位置情報と前記記憶される位置情報とを比較して、両者が一致するとき前記モバイル端末に対し回線への接続許可を与える第 3 の過程と、  
を備えるモバイル端末の接続管理方法。

## 【発明の詳細な説明】

## 【0001】

【発明の技術分野】本発明は、携帯電話機や PHS 端末のようなモバイル端末の接続管理方法及び方式に関するものである。

## 【0002】

【従来の技術】従来、モバイル端末の、リモートアクセスやダイヤルアップ等による LAN（企業内ネットワーク）やインターネット等への接続は、端末所持者の本人確認のため入力要求されたユーザ ID やパスワードが、予め登録されたものと一致したときのみ許可される手法が採用されている。

## 【0003】

【発明が解決しようとする課題】ところで、上記手法においては、ユーザ ID やパスワードを第三者が入手した場合、その第三者が本人になりすまして、自身のモバイル端末を上記 LAN やインターネットに容易に接続することができるとい問題がある。

【0004】また、企業等の従業者が、企業が契約しているユーザ ID に加えて個人で契約しているユーザ ID をも有する場合には、企業内で業務を遂行するときは前者のユーザ ID を、また、自宅等で趣味で利用するときには後者のユーザ ID を夫々意識して使い分ける必要がある。しかし、従業者が不注意により企業のユーザ ID と個人のユーザ ID とを混同して利用したり、或いは、従業者が自宅において上記端末を趣味等で利用しているにも拘らず、故意に企業のユーザ ID を利用してその通話料金を企業に課金するような不正を容易に行えるという問題もあった。

【0005】従って本発明の目的は、端末所持者のユーザ ID やパスワードを不正に入手した第三者による所謂なりすましの接続を防止することができるようにすることにある。

【0006】また、本発明の別の目的は、端末所持者の居場所に応じて使用すべきユーザ ID を自動的に選択することができるようにすることにある。

## 【0007】

【課題を解決するための手段】本発明の第1の側面に従うモバイル端末の接続管理方式は、移動通信網を通じて送信されるモバイル端末の位置情報を受付ける手段と、回線への接続を許可し得るモバイル端末の位置情報を記憶する手段と、受付けた位置情報と記憶される位置情報とを比較して、両者が一致するときモバイル端末に対し回線への接続許可を与える手段とを備える。

【0008】上記構成によれば、受付けた位置情報と記憶される位置情報とを比較して、両者が一致するときモバイル端末に対し回線への接続許可を与えることとしたので、端末所持者のユーザIDやパスワードを不正に入手した第三者による所謂なりすましの接続を防止することができる。

【0009】本発明の第1の側面に係る好適な実施形態では、上述した各手段は、企業内ネットワーク（LAN）を構成するサーバに備えられる。モバイル端末には、携帯電話機や、PHS端末や、モバイルコンピュータが含まれる。上記位置情報は、移動通信網を形成する基地局のゾーンを示すゾーンナンバで表される。このゾーンナンバは、モバイル端末から最寄りの基地局に無線送信されたモバイル端末自身の位置情報に基づき、例えば専用の交換局において生成され、移動通信網を形成する制御局から上述のサーバに送信される。記憶手段には、位置情報と共に、モバイル端末のユーザID、パスワード、移動機IDがテーブル形式で記憶される。接続許可付与手段は、モバイル端末から送信されるユーザID及びパスワードと、記憶されているユーザID及びパスワードとが夫々一致したとき、両位置情報の一致／不一致を判定する。

【0010】本発明の第2の側面に従うモバイル端末の接続管理方式は、移動通信網を通じて送信されるモバイル端末の位置情報を受付ける手段と、回線への接続を許可し得るモバイル端末の位置情報と、それに対応するユーザIDとを、少なくとも1人のユーザに対し2以上記憶する手段と、記憶される位置情報中から受付けた位置情報に一致するものを選択すると共に、その位置情報に対応するユーザIDを、発信時に使用すべきユーザIDとしてモバイル端末に送信する手段とを備える。

【0011】本発明の第2の側面に係る好適な実施形態では、モバイル端末からのパスワードと予め登録されるパスワードとが一致したとき、モバイル端末に対し回線への接続許可を与える手段を更に備える。上述した各手段は、パソコン通信業者又はインターネットの接続プロバイダのホスト装置に備えられる。

【0012】本発明の第3の側面に従うモバイル端末の接続管理方法は、移動通信網を通じて送信されるモバイル端末の位置情報を受付ける第1の過程と、回線への接続を許可し得るモバイル端末の位置情報を記憶する第2の過程と、受付けた位置情報と記憶される位置情報とを

比較して、両者が一致するときモバイル端末に対し回線への接続許可を与える第3の過程とを備える。

## 【0013】

【発明の実施の形態】以下、本発明の実施の形態を、図面により詳細に説明する。

【0014】図1は、本発明の一実施形態に係るモバイル端末としての携帯電話機の接続管理方式が適用される情報通信システムの全体構成を示すブロック図である。

【0015】上記システムは、携帯電話基地局（基地局）1と、無線回線制御局（制御局）3と、携帯電話機（モバイル端末）5と、有線通信回線網（回線網）7と、接続プロバイダのアクセスポイント（アクセスポイント）9と、パソコン通信事業者のアクセスポイント（アクセスポイント）11とを含む。上記システムは、上記各部に加えて更に、インターネット13と、一般家庭に設置されるパソコン端末15、17、及びLAN19をも含む。図1では図示と説明の都合上、基地局は符号1で示した1つだけを記載したが、実際のシステムでは、基地局はサービスエリアの大きさに応じて多数設置されている。また、制御局3や、携帯電話機5や、アクセスポイント9、11や、一般家庭に設置されるパソコン（パーソナルコンピュータ）端末15、17や、LAN19等も実際のシステムでは多数存在する。しかし、上記と同様の理由から、制御局、携帯電話機、アクセスポイント、及びLANについては、夫々符号3、5、9、11、19で示した1つだけを、パソコン端末については、符号13、15を付した2台だけを記載した。基地局1と、制御局3と、携帯電話機5と、回線網7と、図示しない複数の移動通信専用の交換局（専用交換局）とで移動通信網を形成する。

【0016】基地局1は、回線網7において、制御局3、及び専用交換局（図示しない）を通じ通常の交換局（固定電話機用交換局のこと。図示しない）に接続される。基地局1は、そのゾーン内を移動する携帯電話機5に対し、自局の位置登録エリアを示すエリア登録番号情報を報知すべく、上記情報を常時無線送信すると共に、携帯電話機5側から無線送信される位置登録信号を受信する。この位置登録信号は、制御局3を通じて上記ゾーン直属の専用交換局（図示しない）に送出され、その専用交換局において割り出された、携帯電話機5が属する専用交換局（ホームメモリ局という）に送信される。上記信号は、ホームメモリ局において上記移動通信網内をルーティング可能な位置情報に変換されると共に、ホームメモリ局の記憶部に上記携帯電話機5の番号情報に対応させて記憶される。

【0017】携帯電話機5は、自端末（5）内に更新可能に記憶される上記基地局1からのエリア登録番号情報と、現在受信しているエリア登録番号情報とを照合し、両者が不一致のとき、位置登録信号を無線送信する。この信号が基地局1によって受信されると、上述した処理

が実行され、携帯電話機5の新たな位置情報が上記のようにホームメモリ局の記憶部に記憶される。上記一連の処理は位置登録と称される。携帯電話機5は固定電話機と相違して、その現在位置が常時変わるので、位置登録は、携帯電話機5の現在位置を常に明確にしておくことにより、携帯電話機5への着信が不能になる不具合を防止するために必要な処理である。

【0018】制御局3は、各基地局1の位置情報の把握や、携帯電話機5の位置検出制御や、携帯電話機5への着信制御や、携帯電話機5からの発信制御及び位置登録制御や、通話中チャンネル切換制御や、終話切断制御や、無線回線使用状態の管理や、無線区間制御信号の誤り制御等を実行する。

【0019】なお、アクセスポイント9には、ホストコンピュータ（ホスト装置）9aと、WWWサーバ9bが備えられ、アクセスポイント11には、ホスト装置11aと、データベース（DB）11bとが備えられる。また、パソコン端末15は、モデム16及び電話回線18を通じてアクセスポイント9に、パソコン端末17は、モデム20及び電話回線22を通じてアクセスポイント11に、夫々接続される。更に、LAN19は、モデム及びターミナルアダプタ（TA）21や、サーバマシン（サーバ）23や、複数台のパソコン端末25a、25b、25c、・・・や、WWWサーバ27を備える。

【0020】図2は、図1に記載したLAN19のサーバ23に備えられるリモートアクセスユーザ管理テーブルを示す説明図である。

【0021】上記テーブルは、図2に示すように、ユーザID登録エリアと、パスワード登録エリアと、ゾーンナンバ登録エリアと、移動機（携帯電話機）ID登録エリアとを備える。

【0022】ユーザID登録エリアには、例えば1番目のユーザのユーザIDとして「ABC1234」が、2番目のユーザのユーザIDとして「XYZ9876」が、夫々予め登録される。パスワード登録エリアには、例えば上記1番目のユーザのパスワードとして「CDE00」が、上記2番目のユーザのパスワードとして「QRS65」が、夫々予め登録される。また、ゾーンナンバ登録エリアには、例えば上記1番目のユーザによる携帯電話機5の正当な使用が認められるゾーンとして「A」ゾーンが、上記2番目のユーザによる携帯電話機5の正当な使用が認められるゾーンとして「B」ゾーンが、夫々予め登録される。

【0023】更に、移動機ID登録エリアには、例えば上記1番目のユーザの移動機IDとして「030 111 222」が、上記2番目のユーザの移動機IDとして「030 222 333」が、夫々予め登録される。なお、3番目以下のユーザのユーザID、パスワード、ゾーンナンバ、及び移動機IDについては、図示と説明を省略する。

【0024】図3は、図1に記載したシステムにおける携帯電話機5の位置情報の入手経路を示す説明図である。

【0025】図3において、携帯電話機5の位置情報（現在位置情報）は、制御局3により図示しないホームメモリ局から読出され、破線で示すように、アクセスポイント9、11、及びLAN19に夫々送信される。LAN19に送信された上記位置情報は、モデム及びTA21を通じサーバ23によって読込まれる。上記位置情報に対応するゾーンナンバがサーバ23において生成される。このゾーンナンバは、サーバ23がLAN19のリモートアクセスポイントに対する上記携帯電話機5の接続可否の判断を行うに際して上記テーブル中のゾーンナンバ登録エリアのゾーンナンバと比較される。この詳細については、図4で説明する。

【0026】図4は、図1に記載したシステムにおいて、LAN19のリモートアクセスポイントに対する上記携帯電話機5の接続可否の判断を行うに際しての各部の処理動作を示すフローチャートである。

【0027】図4において、携帯電話機5が制御局3の管理下で、基地局1、回線網7、アクセスポイント9（又は11）、及びインターネット13等を通じてLAN19のリモートアクセスポイントに対し接続を要求すると、サーバ23はそれを読込む（ステップS31）。そして、携帯電話機5に対しユーザIDの送信を要求し、その要求に応じて携帯電話機5から送信されたユーザIDを取得すると共に（ステップS32）、パスワードの送信をも要求し、それに応じて携帯電話機5から送信されたパスワードをも取得する（ステップS33）。

【0028】次に、携帯電話機5の現在位置（つまり、携帯電話機5が現在どのゾーンに存在しているか）を示す情報として、ゾーンナンバを取得する（ステップS34）。上記位置登録信号が携帯電話機5から送信された場合には、ホームメモリ局において、その信号を変換して得た上記位置情報が、上記信号が送信されなかったときはホームメモリ局に記憶されている位置情報が、制御局3により読出され（ステップS36、S37）、制御局3からサーバ23へ送信される（ステップS38）。

【0029】次に、サーバ23は、上記テーブルを読出し（ステップS35）、登録されているユーザIDとステップS32で取得したユーザID、登録されているパスワードとステップS33で取得したパスワード、登録されているゾーンナンバとステップS34で取得したゾーンナンバとを夫々比較する（ステップS36）。ここで、上記読込んだユーザID、パスワード、及びゾーンナンバが、夫々「ABC1234」、「CDE00」、及び「A」ゾーン（企業等の事業所外）であったとすれば、これらはいずれも上記テーブル（図2に記載）に登録されている1番目のユーザのものと一致する。よって、サーバ23は、携帯電話機5に対しLAN19のリ

リモートアクセスポイントへの接続を容認する（つまり、リモートアクセスサービスを許可する）（ステップS40）。一方、ステップS36での比較の結果、ユーザID及びパスワードは一致していたが、ゾーンナンバが「A」ではなく例えば「C」であったとすれば、ゾーンナンバが不一致であるので、サーバ23は、携帯電話機5に対しリモートアクセスサービスの提供を拒否する（ステップS41）。

【0030】ここで、例えば正当なユーザが企業等の事業所内（そのゾーンナンバを仮に「F」とする）にいるにも拘らず、所謂なりすましの第三者がLAN19のリモートアクセスポイントに接続しようとしたとする（事業所内にいる正当なユーザが、そのリモートアクセスポイントに接続を試みることは通常あり得ない）。この場合、ステップS36での比較の結果、上記ユーザID及びパスワードは当然一致するが、携帯電話機5の現在位置を示すゾーンナンバは正当なユーザが事業所内にいるため、「F」である。よって、上記テーブル中のゾーンナンバ登録エリアの「A」とは一致しないから、上記第三者によるLAN19のリモートアクセスポイントへの接続は拒否される。

【0031】図5は、図1に記載したシステムにおいて、第三者のモバイル端末が、所謂なりすましによりLAN19のリモートアクセスポイントへの接続を試みようとするときの態様を示す説明図である。

【0032】図5の例では、モバイル端末の一種である、機能的に全く同一のモバイルコンピュータ（所謂ノートブック型パソコン）が、図示と説明の都合上、図1（図2）で記載したLAN19に対するリモートクライアントとして2台存在するものとする。そのうちの1台は、正当なユーザが所持するものであり、便宜上リモートクライアントAで表す。他の1台は、そのユーザのユーザIDやパスワードを不正に入手してそのユーザになりすました第三者が所持するものであり、便宜上リモートクライアントBで表す。

【0033】ここで、リモートクライアントAは、上述した「A」ゾーンに存在しているため、上述したサーバ23には、ゾーンナンバとして「A」が与えられる。よって、リモートクライアントAに対しては、LAN19へのリモートアクセスサービスが許可され、所謂オフィス内クライアントと同様の環境が社外（企業等の事業所外）に形成される。しかし、リモートクライアントBは、上記「A」ゾーン以外のゾーンに存在しているため、サーバ23には、ゾーンナンバとして「A」が与えられない。よって、リモートクライアントBに対しては、LAN19へのリモートアクセスサービスが拒否されることになる。

【0034】なお、ユーザが、LAN19に対するどのようなリモートアクセスも有効にしたいとしないのであれば、携帯電話機5の駆動電源をOFFにすれば、ユーザ

の現在位置がどこであろうとも上記ゾーンナンバ登録エリアのゾーンナンバと一致しないから、LAN19のリモートアクセスポイントに対する全ての接続を拒否することができる。

【0035】図6は、図1に記載したアクセスポイント11のホスト装置（サーバ）11aに備えられるリモートアクセスユーザ管理テーブルの変形例を示す説明図である。

【0036】本変形例は、モバイル端末を業務で使用するため企業等が契約したユーザIDと、モバイル端末を自宅等において趣味で利用するため個人で契約したユーザIDというように、1人のユーザが複数のユーザIDを所有し、上記各ユーザIDを、ユーザが用途に応じて意識して使い分けるような事例に適用される。

【0037】上記のように、用途に応じてユーザが複数のユーザIDを意識的に使い分ける場合には、例えば業務を遂行するためモバイル端末を利用するのに、誤って個人で契約したユーザIDを使用したりする問題が生じる。或いは、自宅等で趣味で利用するのに、故意に業務用のユーザIDを使用してその通話料金を企業等に課金させるようにする等の不正行為が容易に行えるという問題もあった。そこで、本変形例に係る手法を提案するに至ったものである。本変形例の主な特徴は、以下に説明するように、同一のユーザが所有する各ユーザID毎にコールIDを設定し、それらのコールIDをアクセスポイント11側で管理することとした点にある。

【0038】図6に記載するテーブルには、1人のユーザが、所有する複数のユーザIDを始め、それらに対応するパスワードや、ゾーンナンバ等が登録可能なよう、ユーザID登録エリアと、パスワード登録エリアと、ゾーンナンバ登録エリアと、移動機ID登録エリアとが設定される。本変形例では、更に、各ユーザIDに夫々対応させて、複数のコールID登録エリアも設定される。

【0039】図6の例では、ユーザが個人で契約したユーザID（図6の上段側）について、ユーザID登録エリア、パスワード登録エリア、及びゾーンナンバ登録エリアには、夫々図2で記載したのと同じ「ABC1234」、「CDE00」、及び「A」が登録される。一方、企業等が契約したユーザID（図6の下段側）について、ユーザID登録エリア、パスワード登録エリア、及びゾーンナンバ登録エリアには、夫々「FGH8765」、「NOP54」、及び「B」が登録される。更に、図6の上段側のコールID登録エリアには、「12345」が、図6の下段側のコールID登録エリアには、「67890」が、夫々登録される。なお、上記各段の移動機ID登録エリアには、勿論モバイル端末の移動機IDである「030 111 222」が登録される。

【0040】本変形例では、上述した実施形態と異なり、モバイル端末の位置情報ではなく、コールIDが制

御局 3 からホスト装置 11a へ送信される。

【0041】図 7 は、図 1 に記載したシステムにおいて、ユーザがモバイル端末を自宅で利用するとき、企業等において利用するときの態様を示す説明図である。

【0042】図 7 の例では、同一のユーザが同一のモバイル端末 29 を自宅で利用するときは、図示のようにモバイル端末 29 が「A」ゾーン内に存在するから、上記モバイル端末 29 から送信される位置情報は「A」ゾーンに対応したものとなる。この位置情報を受信すると、制御局 3 は、上記「A」ゾーンに対応するコール ID として「12345」をホスト装置 11a に送信する。ホスト装置 11a では、このコール ID と上記テーブル中のコール ID 登録エリアとを比較対照することにより、コール ID 「12345」に対応するゾーンナンバ「A」を取得すると共に、そのゾーンナンバ「A」から上記テーブルを参照してユーザ ID 「ABC1234」を選択する。そして、そのユーザ ID を、上記モバイル端末 29 側に送信すると共に、パスワードの入力を要求する。モバイル端末 29 側から送信されたパスワードが上記パスワード登録エリアの「CDE00」に一致していれば、上記モバイル端末 29 によるアクセスポイント 11 への接続を容認する。

【0043】一方、同一のユーザが同一のモバイル端末 29 を企業内等で利用するときは、図示のようにモバイル端末 29 が「B」ゾーン内に存在するから、上記モバイル端末 29 から送信される位置情報は「B」ゾーンに対応したものとなる。この場合には制御局 3 は、上記「B」ゾーンに対応するコール ID として「67890」をホスト装置 11a に送信する。ホスト装置 11a では、これによりユーザ ID 「FGH8765」を上記モバイル端末 29 側に送信する。以下は上記と同様である。

【0044】図 8 は、図 7 で示した態様における各部の処理動作を示すフローチャートである。

【0045】図 8 において、ユーザがモバイル端末 29 を用いて自宅からアクセスポイント 11 にインターネット 13 への接続を要求すると、ホスト装置 11a はそれを読込む（ステップ S71）。そして、モバイル端末 29 の現在位置を示す情報として、コール ID 「12345」を制御局 3 側から取得する（ステップ S72）。このコール ID は、上述した態様でモバイル端末 29 から送信された位置情報に基づき、上記ホームメモリ局、或いは制御局 3 側で生成され、制御局 3 からホスト装置 11a へ送信される（ステップ S81、S82、S83）。

【0046】次に、ホスト装置 11a は、上記テーブルを読出し（ステップ S73）、上記取得したコール ID 「12345」に対応したモバイル端末 29 のゾーンナンバ（この場合は、ユーザが自宅にいるから「A」である）を上記テーブルから取得する（ステップ S74）。

そして、そのゾーンナンバ「A」に対応するユーザ ID（この場合は、「ABC1234」）を選択すると共に、そのユーザ ID をモバイル端末 29 側へ送信する（ステップ S75）。

【0047】次に、モバイル端末 29 に対しパスワードの送信を要求し、それに応じてモバイル端末 29 から送信されたパスワード「CDE00」を取得すると共に（ステップ S76）、そのパスワードと、ステップ S73 で読み出したテーブル中のパスワード登録エリアに登録されるパスワードとを比較対照する（ステップ S77）。その比較の結果、両者が一致していれば（ステップ S78）、ホスト装置 11a は、モバイル端末 29 に対しインターネット 13 への接続を容認する（ステップ S79）。一方、ステップ S78 での比較の結果、不一致であれば、インターネット 13 への接続を拒否することになる（ステップ S80）。

【0048】なお、ユーザがモバイル端末 29 を用いて企業等からアクセスポイント 11 にインターネット 13 への接続を要求する場合は上記と異なり、コール ID 「67890」、ゾーンナンバ「B」、ユーザ ID 「FGH8765」、及びパスワード「NOP54」が用いられることになる。それ以外は上記と同様である。

【0049】上記構成によれば、ユーザ ID がホスト装置 11a 側からモバイル端末 29 側に送信されるようになっているため、ユーザが自宅にいて企業等が契約したユーザ ID でモバイル端末をインターネット 13 に接続することができない。よって、ユーザがモバイル端末 29 を自宅等で趣味で利用するのに、故意に業務用のユーザ ID を使用してその通話料金を企業等に課金させるようにする等の不正行為が防止される。

【0050】なお、ホスト装置 11a 側からコール ID やユーザ ID 等を通知するのではなく、上述した一実施形態におけるように、ユーザ ID、パスワード、及びゾーンナンバの一致／不一致により、ホスト装置 11a がインターネット 13 への接続の可否を判断するようにしてもよい。

【0051】上述した内容は、あくまで本発明に係る実施形態及びその変形例に関するものであって、本発明が上記内容のみに限定されることを意味する趣旨でないのは勿論である。

【0052】

【発明の効果】以上説明したように、本発明によれば、端末所持者のユーザ ID やパスワードを不正に入手した第三者による所謂なりすましの接続を防止できるようなことができる。

【0053】また、本発明によれば、端末所持者の居場所に応じて使用すべきユーザ ID を自動的に選択できるようにすることができる。

【図面の簡単な説明】

【図 1】本発明の一実施形態に係るモバイル端末として

10

20

30

40

50



の携帯電話機の接続管理方式が適用される情報通信システムの全体構成を示すブロック図。

【図2】図1に記載のLANのサーバに備えられるリモートアクセスユーザ管理テーブルを示す説明図。

【図3】図1に記載のシステムにおける携帯電話機の位置情報の入手経路を示す説明図。

【図4】図1に記載のシステムにおいて、LANのリモートアクセスポイントに対する携帯電話機の接続可否の判断を行うに際しての各部の処理動作を示すフローチャート。

【図5】図1に記載のシステムにおいて、第三者のモバイル端末が、所謂なりすましによりLANのリモートアクセスポイントへ接続を試みようとするときの態様を示す説明図。

【図6】図1に記載のパソコン通信事業者のアクセスポイントのホスト装置に備えられるリモートアクセスユーザ管理テーブルの変形例を示す説明図。

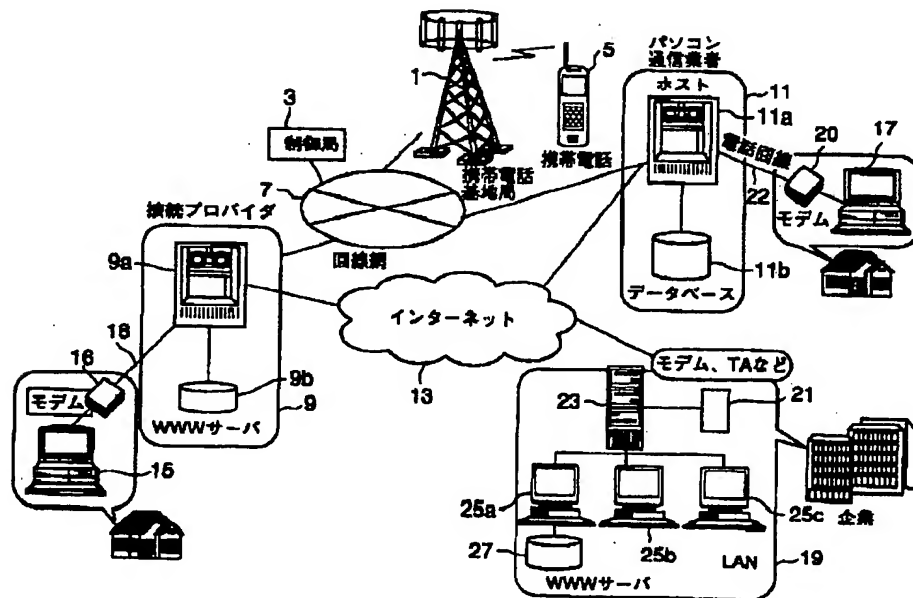
【図7】図1に記載のシステムにおいて、ユーザがモバイル端末を自宅で利用するときと、企業等において利用するときの態様を示す説明図。

【図8】図7で示した態様における各部の処理動作を示すフローチャート。

【符号の説明】

- 1 携帯電話基地局（基地局）
- 3 無線回線制御局（制御局）
- 5 携帯電話機（モバイル端末）
- 7 有線通信回線網（回線網）
- 9 接続プロバイダのアクセスポイント（アクセスポイント）
- 9a、11a ホストコンピュータ（ホスト装置）
- 9b、27 WWWサーバ
- 11 パソコン通信事業者のアクセスポイント（アクセスポイント）
- 11b データベース（DB）
- 13 インターネット
- 15、17 一般家庭に設置されるパソコン（パーソナルコンピュータ）端末
- 16、20 モデム
- 18、22 電話回線
- 19 LAN（企業内ネットワーク）
- 21 モデム及びターミナルアダプタ（TA）
- 23 サーバマシン（サーバ）
- 20 25a、25b、25c パーソナルコンピュータ（パソコン）端末
- 29 モバイル端末（携帯電話機を含む）

【図1】

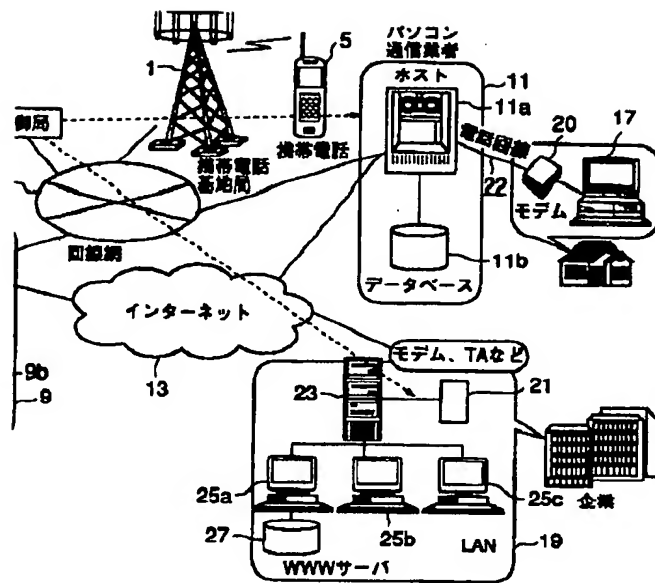




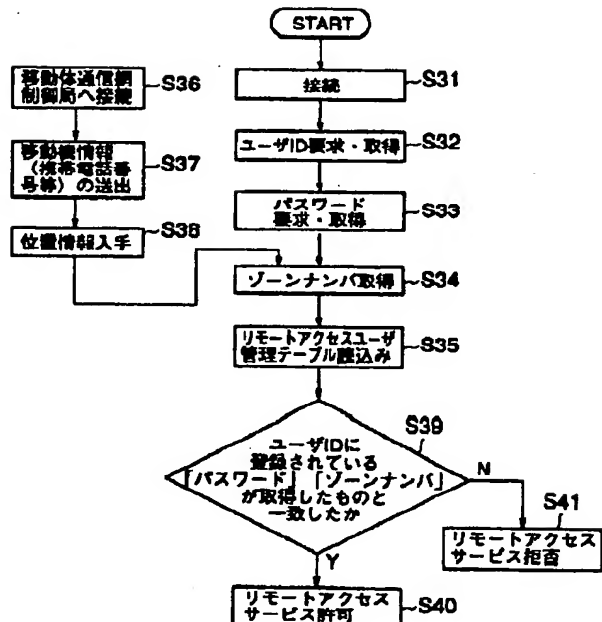
【図2】

	ユーザID	パスワード	ゾーンナンバ	移動機ID
1	ABC1234	CDE00	A	030 111 222
2	XYZ9876	QRS65	B	030 222 333
	⋮	⋮	⋮	⋮

【図3】



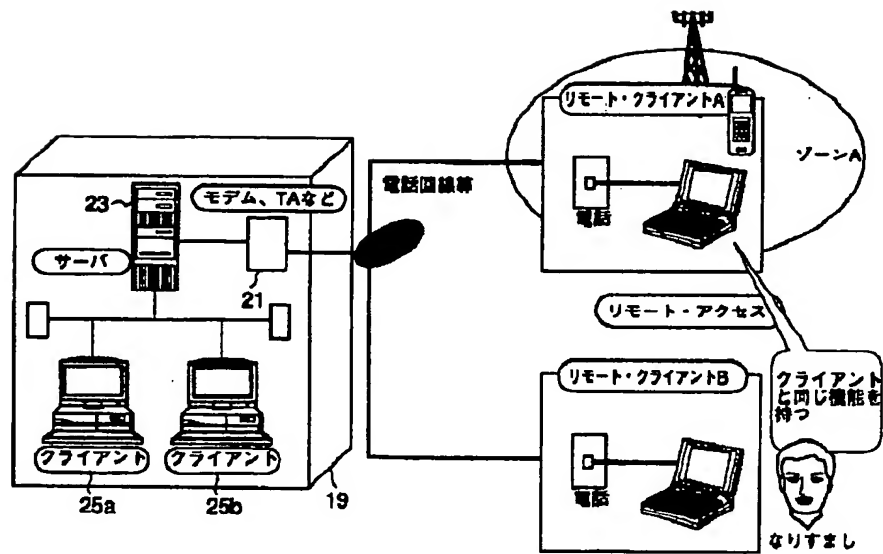
【図4】



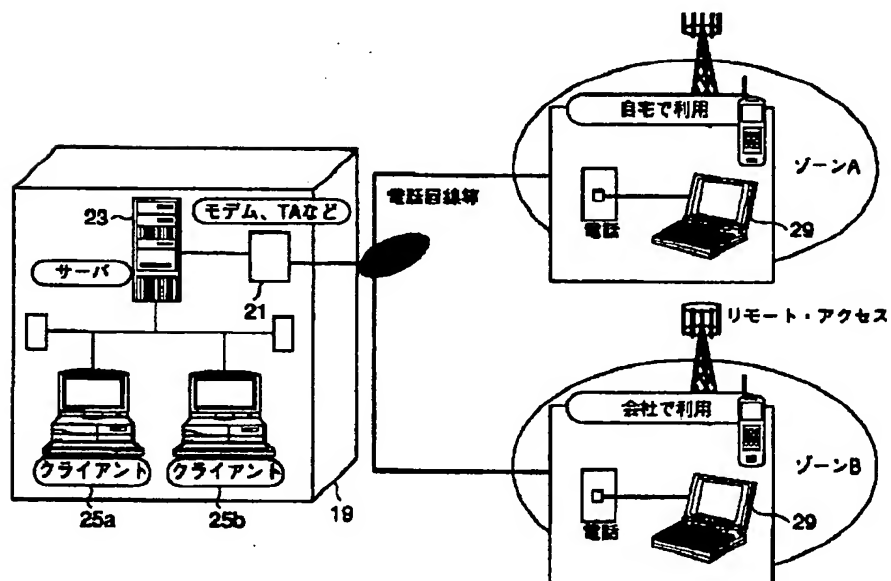
【図6】

	ユーザID	パスワード	ゾーンナンバ	コールID	移動機ID
1	ABC1234	CDE00	A	12345	030 111 222
2	FGH8765	NOP54	B	67890	030 111 222
	⋮	⋮	⋮	⋮	⋮

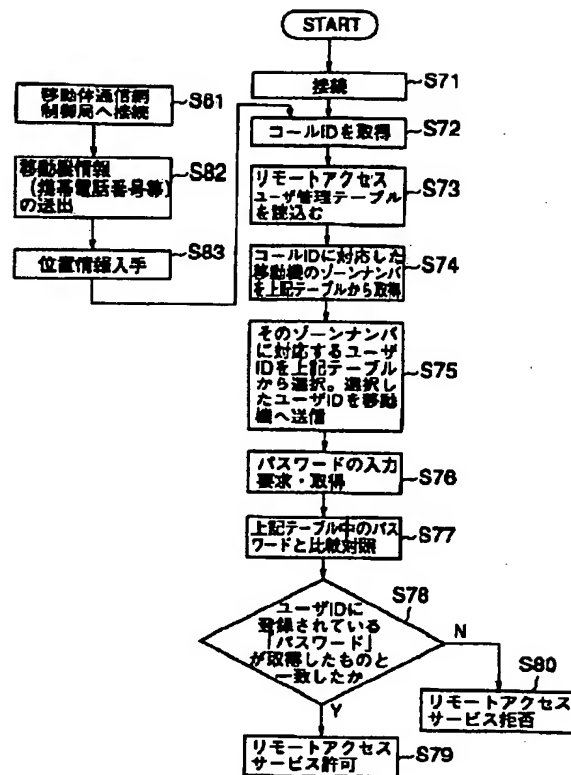
【図 5】



【図 7】



【図8】



フロントページの続き

Fターム(参考) 5K067 AA34 BB04 BB21 DD13 DD17  
 DD19 DD20 EE03 EE10 FF03  
 GG01 GG11 HH05 HH22 HH23  
 HH24 JJ11 JJ21 JJ52 KK15